Cryptographic Protocols on the non-commutative Ring R

AZIZ BOULBOT, ABDELHAKIM CHILLALI, ALI MOUHIB
Sidi Mohamed Ben Abdellah University
Department of Mathematics, Physical and Computer
FP, LSI, Taza
Morocco
aziz.boulbot@usmba.ac.ma
abdelhakim.chillali@usmba.ac.ma

Abstract: In this paper we introduce one of the most famous problems in a non commutative ring R. In particular we are interested in cryptography is mainly encryption based on conjugal classical problem in R. We study the problem of conjugal over this non commutative ring. The problem as stated is generally impossible to solve. Next, we describe a new encryption scheme over this ring based on this problem.

Key–Words: Finite field, Finite ring, Local ring, Cryptography.

1 Introduction

Ever since the discovery of public-key cryptography by Diffie and Hellman in the year 1976 see, [5], the necessity for total privacy of digital data has become stronger and stronger, especially since the internet has become an indispensable part of both our private and work lives. Naturally, the question for more and more secure encryption schemes arose in the past few decades. One way to achieve confidentiality in applications, such as online banking, electronic voting, virtual networks etc , are homomorphic and especially fully homomorphic cryptographic schemes. Fully homomorphic cryptosystems or privacy homomorphisms were introduced by Rivest, Adleman, and Dertouzous in 1978 see, [6] . In their paper they asked for a way to allow a third, untrusted party to carry out extensive computation on encrypted data, without having to decrypt first. Unfortunately, shortly after its publication, major security as were found in the original proposed schemes of Rivest and al. The search for fully homomorphic cryptosystems began. The aim of homomorphic cryptography is to ensure privacy of data in communication and storage processes, such as the ability to delegate computations to untrusted parties. If a user could take a problem defined in one algebraic system and encode it into a problem in a different algebraic system in a way that decoding back to the original algebraic system is hard, then the user could encode expensive computations and send them to the untrusted party. This untrusted party then performs the corresponding computation in the second algebraic system, returning the result to the user. Upon receiving the result, the user can decode it into a solution in the original algebraic system, while the untrusted party learns nothing of which computation was actually performed. Asked: ”Is there an encryption function Enc() such that both $Enc(x + y)$ and $Enc(x.y)$ are easy to compute from $Enc(x)$ and $Enc(y)$?”

Definition 1 *A public-key encryption scheme E is a tuple, (K, E, D) of probabilistic polynomial-time algorithms*
(1) The key generation algorithm K takes the security parameter k as input and outputs a pair of keys (pk, sk). I refer to the first of these as the public key and the second as the private key or secret key. I assume that pk and sk each have length at least k, and that k can be determined from pk, sk.
(2) The encryption algorithm E takes a public-key pk and a string m called the message from some underlying message space M as input. It produces a cipher text c from an underlying cipher text space C, denoted as $c = Encpk(m)$ or simple $c = Enc(m)$, if it is obvious which public key is in use.
(3) The decryption algorithm D takes a private-key sk and a cipher text c as input, and produces an output message m. Without loss of generality we assume that Dec is deterministic, and write this as $m := Decsk(c)$.

2 Definitions and Notation

Let d be a positive integer and $q = p^d$ be a power of a prime number $p \geq 5$. Let $\mathbf{F}_q$ a finite field of characteristic p and order q. We define the set $\mathbf{F}_q[e], e^2 = e$ as:

$$\mathbf{F}_q[e] := \{\alpha + \beta e | (\alpha, \beta) \in \mathbf{F}_q \times \mathbf{F}_q \ \texttt{and}\ e^2 = e\}.$$

We define on the set $\mathbf{F}_q[e]$ the laws some "+" and product "." by:
Let $X = \alpha_0+\beta_0 e \in \mathbf{F}_q[e]$ and $Y = \alpha_1+\beta_1 e \in \mathbf{F}_q[e]$:

$$\begin{cases} X+Y = (\alpha_0+\alpha_1)+(\beta_0+\beta_1)e \\ X.Y = (\alpha_0\alpha_1)+(\alpha_0\beta_1+\alpha_1\beta_0+\beta_0\beta_1)e \end{cases}$$

We have:
$\Big(\mathbf{F}_q[e],+,.\Big)$ is a finite unitary commutative ring.[2, 3]

Definition 2 *We define an elliptic curve over the ring $\mathbf{F}_q[e]$, as a curve in $\mathbf{P}^2\Big(\mathbf{F}_q[e]\Big)$ which is given by the Weierstrass equation:*

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $\mathbf{P}^2\Big(\mathbf{F}_q[e]\Big)$ is the projective space over $\mathbf{F}_q[e]$ and $a, b \in \mathbf{F}_q[e]$ such that the discriminant $\Delta := 4a^3 + 27b^2$ is invertible in $\mathbf{F}_q[e]$.

Notation 3 *Let $a, b \in \mathbf{F}_q[e]$. If the discriminant $\Delta = 4a^3+27b^2$ is invertible in $\mathbf{F}_q[e]$, we denote the elliptic curve over $\mathbf{F}_q[e]$ by $E_{a,b}\Big(\mathbf{F}_q[e]\Big)$, and we write:[1]*

$$E_{a,b}\Big(\mathbf{F}_q[e]\Big) = \Big\{[X:Y:Z] \in \mathbf{P}^2\Big(\mathbf{F}_q[e]\Big) \Big/ Y^2Z = X^3+aXZ^2+bZ^3\Big\}$$

3 The Ring R

In this section, $E_{a,b}\Big(\mathbf{F}_q[e]\Big)$ is an elliptic curve over $\mathbf{F}_q[e]$, P is a point of order n and G is the group generated by P. We consider the set:

$$R = \{\begin{pmatrix} x & tP \\ 0 & y \end{pmatrix} | x, y, t \in \{0, ..., n-1\}\}$$

Let $X = \begin{pmatrix} x & tP \\ 0 & y \end{pmatrix}$ and $Y = \begin{pmatrix} z & rP \\ 0 & w \end{pmatrix}$ are two elements in R, on which two binary operations are defined, called addition $(+)$ and start $(*)$ and denoted by:

$$X+Y = \begin{pmatrix} x+z & (t+r)P \\ 0 & y+w \end{pmatrix}$$

$$X*Y = \begin{pmatrix} xz & (tw+xr)P \\ 0 & yw \end{pmatrix}$$

Lemma 4 *$(R, +, *)$ is a non commutative ring with identity $1_R = \begin{pmatrix} 1 & [0:1:0] \\ 0 & 1 \end{pmatrix}$.*

Proof: $(R, +, *)$ is called a non commutative ring with respect to these operations, if the following properties hold:

- ○ Associative laws: $\forall X, Y, Z \in R$,

$$(X+Y)+Z = X+(Y+Z)$$

$$(X*Y)*Z = X*(Y*Z)$$

- ○ Commutative law: $\forall X, Y \in R$,

$$X+Y = Y+X$$

- ○ A non commutative law: $\exists X, Y \in R$ such that

$$X*Y \neq Y*X$$

- ○ Distributive laws: $\forall X, Y, Z \in R$,

$$(X+Y)*Z = X*Z+Y*Z$$

$$Z*(X+Y) = Z*X+Z*Y$$

- ○ Additive identity: $\forall X \in R$,

$$X+0_R = 0_R+X = X$$

where $0_R = \begin{pmatrix} 0 & [0:1:0] \\ 0 & 0 \end{pmatrix}$ is called the additive identity element of R.

- ○ Start identity: $\forall X \in R, X*1_R = 1_R*X = X$, 1_R is called the start identity element of R.
- ○ Additive inverses: $\forall X \in R, X+(-X) = 0_R$; $-X$ is called the additive inverse of X.

□

Lemma 5 *Let $X = \begin{pmatrix} x & Q \\ 0 & y \end{pmatrix} \in R$.*
X is invertible if only if $x \wedge n = 1$ and $y \wedge n = 1$, in this case we have :

$$X^{-1*} = \begin{pmatrix} x^{-1} & -x^{-1}y^{-1}Q \\ 0 & y^{-1} \end{pmatrix}$$

Proof: Let $Y = \begin{pmatrix} z & R \\ 0 & w \end{pmatrix}$ the inverse of X, we have:

$$X*Y = Y*X = 1_R$$

So,
$X*Y = \begin{pmatrix} xz & xR+wQ \\ 0 & yw \end{pmatrix} = \begin{pmatrix} 1 & [0:1:0] \\ 0 & 1 \end{pmatrix}$
and
$Y*X = \begin{pmatrix} xz & yR+zQ \\ 0 & yw \end{pmatrix} = \begin{pmatrix} 1 & [0:1:0] \\ 0 & 1 \end{pmatrix}$,

thus $$\begin{array}{rcl} xz & = & 1[n] \\ yw & = & 1[n] \\ xR+wQ & = & [0:1:0] \\ yR+zQ & = & [0:1:0] \end{array}$$
Therefore, X is invertible if only if $x \wedge n = 1$ and $y \wedge n = 1$, in this case we have:

$$R = -x^{-1}wQ = -y^{-1}zQ = -x^{-1}y^{-1}Q$$

so,

$$X^{-1*} = \begin{pmatrix} x^{-1} & -x^{-1}y^{-1}Q \\ 0 & y^{-1} \end{pmatrix}$$

Lemma 6 *Let k be a strictly positive integer. Then if $X = \begin{pmatrix} x & Q \\ 0 & y \end{pmatrix}$ is any element of R. The k-power of X can be given by $X^k = \begin{pmatrix} x^k & \alpha_k Q \\ 0 & y^k \end{pmatrix}$, where $\alpha_k = \sum_{i+j=k-1} x^i y^j$*

Proof: Using a proof is by induction on k.
For $k = 1$: we have $\alpha_1 = 1$.
Let $k \geq 1$. Assume that, $\alpha_k = \sum_{i+j=k-1} x^i y^j$ and proof that: $\alpha_{k+1} = \sum_{i+j=k} x^i y^j$, we have:

$$X^{k+1} = \begin{pmatrix} x^k & \alpha_k Q \\ 0 & y^k \end{pmatrix} * \begin{pmatrix} x & Q \\ 0 & y \end{pmatrix}$$

so,

$$X^{k+1} = \begin{pmatrix} x^{k+1} & x^kQ + y\alpha_k Q \\ 0 & y^{k+1} \end{pmatrix}$$

Thus,

$$\alpha_{k+1} = x^k + y\alpha_k = x^k + y \sum_{i+j=k-1} x^i y^j = \sum_{i+j=k} x^i y^j$$

We conclude that, $\forall k \geq 1; \alpha_k = \sum_{i+j=k-1} x^i y^j$ □

4 Cryptographic Protocols

This section describes some, public-key encryption, and key establishment schemes. Surveys the state-of-the-art in algorithms for solving conjugal classical problem in R, whose intractability is necessary for the security of R cryptographic schemes.

4.1 Public-key encryption

Definition 7 *A public-key encryption scheme consists of four algorithms:*
1) A domain parameter generation algorithm that generates a set D of domain parameters.
2) A key generation algorithm that takes as input a set D of domain parameters and generates key pairs (K, d).
3) An encryption algorithm that takes as input a set of domain parameters D, a public key K, a plain text message m, and produces a cipher text c.
4) A decryption algorithm that takes as input the domain parameters D, a private key d, a cipher text c, and either rejects c as invalid or produces a plain text m. The decryption algorithm always accepts (D, d, c) and outputs m if c was indeed generated by the encryption algorithm on input (D, Q, m). [4]

4.2 Description of Cryptosystem Based on R

The purpose of a key establishment protocol is to provide two or more entities communicating over an open network with a shared secret key. The key may then be used in a symmetric-key protocol to achieve some cryptographic goal such as confidentiality or data integrity. A key transport protocol is a key establishment protocol where one entity creates the secret key and securely transfers it to the others. We will consider two-party key agreement protocols derived from the basic Diffie-Hellman protocol. Alice and Bob chooses a ring R and a secret key: K. The secret key consists of an invertible element in R. To encrypt a message m in R, Alice calculate

$$c = e_K(m) = K * m * K^{-1*}.$$

To decrypt a cipher text c, Bob calculate

$$m = d_K(c) = K^{-1*} * c * K.$$

Cryptosystem Based on R:

- ○ Space of lights: $L = R$
- ○ Space of quantified: $C = R$
- ○ Space of keys: R^*
- ○ Function of encryption:$\forall K \in R^*$

$$\begin{array}{rcl} e_K : L & \to & C \\ m & \mapsto & K * m * K^{-1*} \end{array}$$

- ○ Function of decryption:$\forall K \in R^*$

$$\begin{array}{rcl} d_K : C & \to & L \\ c & \mapsto & K^{-1*} * c * K \end{array}$$

We have: $d_K o e_K(m) = m$.

Definition 8 *A public-key encryption scheme $E = (K, E, D)$ is homomorphic if for all k and all (pk, sk) output from k, it is possible to define groups M, C so that:*

1) The plain text space M, and all cipher texts output by $Encpk$ are elements of C.
2) For any $m_1, m_2 \in M$ and $c_1, c_2 \in C$ with $m_1 = Decsk(c_1)$ and $m_2 = Decsk(c_2)$ it holds that: $Decsk(c_1 * c_2) = m_1 * m_2$

A fully homomorphic encryption scheme can be defined as a tuple of three algorithms $E = (K, E, D)$ for which the message space is a ring $(R, +, .)$ and the cipher text space is also a ring $(R', +, .)$ such that for all messages $m_1, m_2 \in R$, and all outputs $(pk, sk) \in K$, we have:

○ $m_1 + m_2 = Decsk(Encpk(m_1, pk) + Encpk(m_2, pk), sk)$

○ $m_1.m_2 = Decsk(Encpk(m_1, pk).Encpk(m_2, pk), sk)$

If E is a symmetric fully homomorphic encryption scheme, we will have a single key for encryption and decryption, so the role of pk will be played by sk. A scheme is supposed to be some what homomorphic if it permits only a limited number of additions and multiplications.
The scheme is constructed using the non commutative ring $(R, +, *)$. The secret key consists of a start invertible element $K \in R$. To encrypt a message $m \in R$, the cipher text $e_K(m)$ is an element $c \in R$ such that: $c = e_K(m)$. To decrypt a cipher text c, we compute: $m = d_k(c)$. This cryptosystem is a fully homomorphic encryption scheme because we have:

○ $e_K(m_1) + e_K(m_2) = K * m_1 * K^{-1*} + K * m_2 * K^{-1*} = e_K(m_1 + m_2)$

○ $e_K(m_1) * e_K(m_2) = K * m_1 * K^{-1*} * K * m_2 * K^{-1*} = e_K(m_1.m_2)$

4.3 Security

The development of quantum computation casts serious threats to the securities of most existing public-key cryptosystems. The cryptography based on this ring R is one of the alternatives that have potential advantages in resisting quantum attacks. In this paper, the state of the art of cryptography based on R is surveyed, and then a new cryptographic problemconjugate adjoining problem related to R rings is proposed. Based on this problem, we design a new encryption scheme. This scheme is efficient and provably secure in the random oracle model. Further, we present the comparison between new signatures schemes and RSA-based ones. The signing process of the R rings-based schemes is more efficient than that of RSA-based ones, while the verifying process of the R rings-based ones is observably slow. Hence, R rings-based signatures are suitable for scenarios where the signing process has to be as quick as possible but delays are permitted in the verifying process, for example, in off-line e-cash systems. The capability of R rings cryptosystems to resist currently known quantum attacks is also discussed from the perspective of hidden subgroup problems.

5 Conclusion

The results explained in the previous sections show that the methode in cryption and decryption on new Ring R based on the conjugacy search problem for a noncommutative Ring . This cryptosystem is a fully homomorphic encryption scheme.

Acknowledgements: The research was supported by the University of Sidi Mohamed Ben Abdellah, FP, LSI.

References:

[1] W. Bosma and H.W. Lenstra , Complete System of Two Addition Laws for Elliptic Curves, *Journal of Number Theory.* 1995

[2] A. Chillali , *Elliptic Curves of the Ring* $\mathbf{F}_q[\varepsilon]$, $\varepsilon^n = 0$, International Mathematical Forum, 2011

[3] M. H. Hassib, A. Chillali and M. Abdou ELOMARY, Special Ideal Ring A_3 and Cryptography, *IEEE.* 2013

[4] N. Koblitz, Elliptic curve cryptosystems, *Math. Compute.* 1987

[5] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory.* 22(6), 1976, pp. 644-654.

[6] R.L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM.* 21(2), 1978, pp. 120-126.